Cost of quantum secret key

arXiv:2402.17007

Karol Horodecki, **Leonard Sikorski**, Sidharta Das, Mark M. Wilde

Quantum Resources, Jeju, 17 – 21 March 2025

NATIONAL SCIENCE CENTRE POLAND

Uniwersytet Gdański

Resource distillation and dilution

Distillation

$$\rho^{\otimes n} \xrightarrow{\text{free operations}} \Phi^{\otimes m}$$

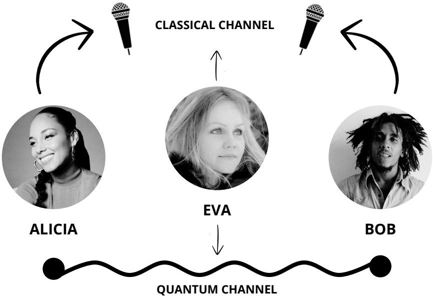
Asymptotic rate measured by R_D

Dilution

$$\Phi^{\otimes m} \xrightarrow{\text{free operations}} \rho^{\otimes n}$$

Asymptotic rate measured by R_C

Quantum cryptography 101



Objects: ρ_{AB}
Operations: LOCC
Target: $\tau|\Phi_+\rangle\langle\Phi_+|_{A_K B_K} \otimes \sigma_{A_S B_S}\tau^\dagger$

Motivating development of resource theory of quantum secret key

- Entanglement is closely related to quantum cryptography...

  ...but they are not equivalent.

- Resource theory of entanglement is well developed...

  ...which is not true for the theory of quantum secret key.

Resource theory of quantum secret key - free states

- $\sigma \in \mathrm{SEP} \Rightarrow K_D(\sigma) = 0$
- Does the converse implication holds?

IQOQI Vienna problem, no. 24 - Secret key from all entangled states

Can all bipartite entangled states be used to generate secret keys?

So... does the converse implication holds?

Our assumption

Assumption

$$K_D(\sigma) = 0 \Rightarrow \sigma \in \mathrm{SEP}$$

Comment: different approach - Stefan Bäuml in his Master Thesis

Outlook on the resource theory of entanglement

- $E_C = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$ (characterization of entanglement cost)
- there exist states for which $E_C > E_D$ (irreversibility)
- for pure states $E_C = E_F = E_D = S_A = E_{sq}$ (reversibility)
- $E_D^{\varepsilon_1} \leq E_C^{\varepsilon_2} + \log_2\left(\frac{1}{1-(\sqrt{\varepsilon_1}+\sqrt{\varepsilon_2})^2}\right)$ (yield-cost relation)

What about the quantum secret key?

Private states

Definition

Private states are bipartite quantum states having the following structure

$$\gamma_{d_k}(\Phi^+) := \tau(\Phi^+_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger,$$

where $|\Phi^+\rangle_{A_K B_K} := \frac{1}{\sqrt{d_k}} \sum_{i=0}^{d_k-1} |ii\rangle_{A_K B_K}$ and $\tau := \sum_{i=0}^{d_k-1} |ii\rangle\langle ii|_{A_K B_K} \otimes U_i^{A_S B_S}$ is a "twisting" operator.

Definition

Generalized private states are bipartite quantum states having the following structure

$$\gamma(\psi) := \tau(\psi_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger,$$

where $|\psi_{A_K B_K}\rangle := \sum_i \lambda_k |e_i\rangle_{A_K} |f_i\rangle_{B_K}$ and $\tau := \sum_i |e_i f_i\rangle\langle e_i f_i|_{A_K B_K} \otimes U_i^{A_S B_S}$ is a "twisting" operator.

Private states

Definition

Private states are bipartite quantum states having the following structure

$$\gamma_{d_k}(\Phi^+) := \tau(\Phi^+_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger,$$

where $|\Phi^+\rangle_{A_K B_K} := \frac{1}{\sqrt{d_k}} \sum_{i=0}^{d_k-1} |ii\rangle_{A_K B_K}$ and $\tau := \sum_{i=0}^{d_k-1} |ii\rangle\langle ii|_{A_K B_K} \otimes U_i^{A_S B_S}$ is a "twisting" operator.

Definition

Generalized private states are bipartite quantum states having the following structure

$$\gamma(\psi) := \tau(\psi_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger,$$

where $|\psi_{A_K B_K}\rangle := \sum_i \lambda_k |e_i\rangle_{A_K} |f_i\rangle_{B_K}$ and $\tau := \sum_i |e_i f_i\rangle\langle e_i f_i|_{A_K B_K} \otimes U_i^{A_S B_S}$ is a "twisting" operator.

Private states

Definition

Private states are bipartite quantum states having the following structure

$$\gamma_{d_k}(\Phi^+) := \tau(\Phi^+_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger,$$

where $|\Phi^+\rangle_{A_K B_K} := \frac{1}{\sqrt{d_k}} \sum_{i=0}^{d_k-1} |ii\rangle_{A_K B_K}$ and $\tau := \sum_{i=0}^{d_k-1} |ii\rangle\langle ii|_{A_K B_K} \otimes U_i^{A_S B_S}$ is a "twisting" operator.

Definition

Generalized private states are bipartite quantum states having the following structure

$$\gamma(\psi) := \tau(\psi_{A_K B_K} \otimes \rho_{A_S B_S})\tau^\dagger,$$

where $|\psi_{A_K B_K}\rangle := \sum_i \lambda_k |e_i\rangle_{A_K} |f_i\rangle_{B_K}$ and $\tau := \sum_i |e_i f_i\rangle\langle e_i f_i|_{A_K B_K} \otimes U_i^{A_S B_S}$ is a "twisting" operator.

Irreducibility of private states

Definition

Irreducible private states: (IR) those private states for which $K_D(\gamma_{d_k}(\Phi^+)) = \log d_k$.

Definition

Strictly irreducible private states: (SIR) those irreducible private states which become separable after the measurement of a key part.

Comment: With our assumption ($K_D(\sigma) = 0 \iff \sigma \in \text{SEP}$), we have IR = SIR.

Definition - Cost of a quantum secret key

Definition (Key cost)

The asymptotic key cost $K_C(\rho)$ and one-shot key cost $K_C^{\varepsilon}(\rho)$ of a state ρ_{AB} are defined as

$$K_C(\rho) := \sup_{\varepsilon \in (0,1)} \limsup_{n\to\infty} \frac{1}{n} K_C^{\varepsilon}(\rho^{\otimes n}),$$

$$\textit{where } K_C^{\varepsilon}(\rho) := \inf_{\substack{\mathcal{L}\in \mathrm{LOCC},\\ \gamma_d \in \mathrm{SIR}}} \left\{ \log_2 d : \frac{1}{2}\|\mathcal{L}(\gamma_d) - \rho\|_1 \le \varepsilon \right\}.$$

$$\gamma_d \xrightarrow{\mathcal{L}\in\mathrm{LOCC}} \mathcal{L}(\gamma_d) \approx_{\varepsilon} \rho^{\otimes n}$$

Definition - Key of formation

Definition (Entanglement of formation)

$$E_F(\rho_{AB}) := \inf_{\sum_{k=1}^{K} p_k |\psi_k\rangle\langle\psi_k| = \rho} \sum_{k=1}^{K} p_k S_A[\psi_k]$$

Definition (Key of formation)

The key of formation of a bipartite state ρ:

$$K_F(\rho) := \inf_{\sum_{k=1}^{K} p_k \gamma(\psi_k) = \rho} \sum_{k=1}^{K} p_k S_{A_K}[\gamma(\psi_k)],$$

where $\gamma(\psi_k)$ are strictly irreducible generalized private state

Definition - Key of formation

Definition (Entanglement of formation)

$$E_F(\rho_{AB}) := \inf_{\sum_{k=1}^K p_k |\psi_k\rangle\langle\psi_k| = \rho} \sum_{k=1}^K p_k S_A[\psi_k]$$

Definition (Key of formation)

The key of formation of a bipartite state ρ:

$$K_F(\rho) := \inf_{\sum_{k=1}^K p_k \gamma(\psi_k) = \rho} \sum_{k=1}^K p_k S_{A_K}[\gamma(\psi_k)],$$

where $\gamma(\psi_k)$ are strictly irreducible generalized private state

Definition - Key of formation

Definition (Entanglement of formation)

$$E_F(\rho_{AB}) := \inf_{\sum_{k=1}^{K} p_k |\psi_k\rangle\langle\psi_k| = \rho} \sum_{k=1}^{K} p_k S_A[\psi_k]$$

Definition (Key of formation)

The key of formation of a bipartite state ρ:

$$K_F(\rho) := \inf_{\sum_{k=1}^{K} p_k \gamma(\psi_k) = \rho} \sum_{k=1}^{K} p_k S_{A_K}[\gamma(\psi_k)],$$

where $\gamma(\psi_k)$ are strictly irreducible generalized private state

Mathematical properties of key of formation

Reminder (Key of formation)

$$K_F(\rho) := \inf_{\sum_{k=1}^{K} p_k \gamma(\psi_k)=\rho} \sum_{k=1}^{K} p_k S_{A_K}[\gamma(\psi_k)],$$

K_F is:

- convex,
- subadditive,
- non-increasing under LOCC on pure states ($K_F = E_F$ for pure states),
- non-increasing under: local unitary transformation, addition of local ancilla and random unitary channels,
- if K_F is non-increasing under LOCC operation Λ on GSIR, then it is non-increasing under Λ in general,

But...

Mathematical properties of key of formation??

Reminder (Key of formation)

$$K_F(\rho) := \inf_{\sum_{k=1}^{K} p_k \gamma(\psi_k)=\rho} \sum_{k=1}^{K} p_k S_{A_K}[\gamma(\psi_k)]$$

We don't know if

$$K_F(\sum_k p_k \sigma_k \otimes |k\rangle\langle k|) \overset{???}{\geq} \sum_k p_k K_F(\sigma_k).$$

So... we don't know if it is an entanglement monotone.

Results from entanglement theory

- $E_C = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$ (characterization of entanglement cost)
- there exist states for which $E_C > E_D$ (irreversibility)
- for pure states $E_C = E_F = E_D = S_A = E_{sq}$ (reversibility)
- $E_D^{\varepsilon_1} \leq E_C^{\varepsilon_2} + \log_2\left(\frac{1}{1-(\sqrt{\varepsilon_1}+\sqrt{\varepsilon_2})^2}\right)$ (yield-cost relation)

Partial characterization of a key cost

Result

Regularized key of formation upperbound key cost,
$K_C(\rho) \leq K_F^{\infty}(\rho) := \lim_{n\to\infty} \frac{1}{n} K_F(\rho^{\otimes n})$

Comment: To obtain this result we developed a Privacy Dilution Protocol.

$$\gamma_d \xrightarrow{\mathcal{L}\in\text{LOCC}} \mathcal{L}(\gamma_d) \approx_{\varepsilon} \rho^{\otimes n}$$

Results from entanglement theory

- $E_C = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$ (characterization of entanglement cost)
- there exist states for which $E_C > E_D$ (irreversibility)
- for pure states $E_C = E_F = E_D = S_A = E_{sq}$ (reversibility)
- $E_D^{\varepsilon_1} \leq E_C^{\varepsilon_2} + \log_2 \left(\frac{1}{1-(\sqrt{\varepsilon_1}+\sqrt{\varepsilon_2})^2} \right)$ (yield-cost relation)

Irreversibility

Result

Regularized entropy of entanglement lowerbounds key cost,
$K_C(\rho) \geq \lim_{n\to\infty} \frac{1}{n} E_R(\rho^{\otimes n}) =: E_R^\infty(\rho)$.

Consequence: for so called *antisymmetric* states[1] $\widehat{\rho}$ there is

$$K_D(\widehat{\rho}) \underbrace{\leq}_{\text{this is known}} E_{\text{sq}}(\widehat{\rho}) \underbrace{<}_{\text{this is know}} E_R^\infty(\widehat{\rho}) \underbrace{\leq}_{\text{this is our result}} K_C(\widehat{\rho}),$$

$$\Downarrow$$

$$\underbrace{K_D(\widehat{\rho}) < K_C(\widehat{\rho})}_{\text{irreversibility}}$$

[1] Christandl, Matthias, Norbert Schuch, and Andreas Winter. "Entanglement of the antisymmetric state." Communications in Mathematical Physics 311.2 (2012): 397-422.

Results from entanglement theory

- $E_C = \lim_{n \to \infty} \frac{1}{n} E_F(\rho^{\otimes n})$ (characterization of entanglement cost)
- there exist states for which $E_C > E_D$ (irreversibility)
- for pure states $E_C = E_F = E_D = S_A = E_{sq}$ (reversibility)
- $E_D^{\varepsilon_1} \leq E_C^{\varepsilon_2} + \log_2 \left(\frac{1}{1-(\sqrt{\varepsilon_1}+\sqrt{\varepsilon_2})^2} \right)$ (yield-cost relation)

Reversibility

Result

For a strictly irreducible generalized private state $\gamma(\psi)_{A_K A_S B_K B_S}$, the following equalities hold: $K_C(\gamma) = K_D(\gamma) = K_F(\gamma) = K_F^{\infty}(\gamma) = S_{A_K}(\gamma) = S_{A_K}(\psi)$.

Results from entanglement theory

- $E_C = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$ (characterization of entanglement cost)
- there exist states for which $E_C > E_D$ (irreversibility)
- for pure states $E_C = E_F = E_D = S_A = E_{sq}$ (reversibility)
- $E_D^{\varepsilon_1} \leq E_C^{\varepsilon_2} + \log_2\left(\frac{1}{1-(\sqrt{\varepsilon_1}+\sqrt{\varepsilon_2})^2}\right)$ (yield-cost relation) [2]

[2] Mark M Wilde. Second law of entanglement dynamics for the non-asymptotic regime. In 2021 IEEE Information Theory Workshop (ITW), pages 1–6. IEEE, 2021.

Yield-cost relation

Result

For every bipartite state ρ and $\varepsilon_1, \varepsilon_2 \in [0,1]$ such that $\varepsilon_1 + \varepsilon_2 < 1$, the following inequality holds:
$K_D^{\varepsilon_2}(\rho) \leq K_C^{\varepsilon_1}(\rho) + \log_2\left(\frac{1}{1-(\varepsilon_1+\varepsilon_2)}\right)$.

Comment: This is not a trivial consequence of a general result [3]

[3] Ryuji Takagi, Bartosz Regula, and Mark M Wilde. One-shot yield-cost relations in general quantum resource theories. PRX Quantum, 3(1):010348, 2022.

Outlook

This is well known	This is new
$E_C = \lim_{n\to\infty} \frac{1}{n} E_F(\rho^{\otimes n})$	$K_C \leq \lim_{n\to\infty} \frac{1}{n} K_F(\rho^{\otimes n})$
$E_C > E_D$ for some states	$K_C > K_D$ for some states
for pure states $E_C = E_F = E_D = S_A = E_{sq}$	for GSIR states $K_C = K_D = K_F = K_F^{\infty} = S_{A_K}$
$E_D^{\varepsilon_1} \leq E_C^{\varepsilon_2} + \log_2\left(\frac{1}{1-(\sqrt{\varepsilon_1}+\sqrt{\varepsilon_2})^2}\right)$	$K_D^{\varepsilon_2}(\rho) \leq K_C^{\varepsilon_1}(\rho) + \log_2\left(\frac{1}{1-(\varepsilon_1+\varepsilon_2)}\right)$

Open problems

- Is K_F and entanglement monotone?
- Is K_F asymptotically continuous?
- Does the equality $K_C = K_F^{\infty}$ hold?

Last slide

Thank you for your attention
:D
감사합니다